IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF MISSISSIPPI
OXFORD DIVISION

TRACY COATES, Plaintiff, vs. SAIA MOTOR FREIGHT LINE, LLC, a/k/a SAIA LTL FREIGHT, MARCUS MORROW, and JOHN DOES 1-10, Defendants.	)	No. 3:20-CV-25-DMB-RP JURY DEMANDED

SUPPLEMENTAL REPORT OF EXAMINATION

INTRODUCTION

Verity LLC., DBA Verity Digital Forensics ("Verity"), was engaged by attorney Earl Houston ("Counsel") of Martin Tate Morrow & Marston P.C., to provide assistance with electronic discovery through forensic analysis of a mobile cellular phone in the matter of **3:20-CV-25-DMB-RP Tracy Coates v Saia Motor Freight Line, LLC, et al.** on behalf of the Defendants.

This report supplements my REPORT OF EXAMINATION issued on September 9, 2020 and addresses issues raised by Plaintiff's expert Larry Daniel of Envista Forensics in his report published on October 13, 2020.

EXECUTIVE SUMMARY

Though the Cellebrite Advanced Logical extraction I originally obtained with the assistance of One Source Discovery (Louisville, KY) has long been the traditional method of forensically preserving an Apple iPhone that is not jailbroken, Plaintiff's expert alleges that a newer method of extraction, a full file system extraction based on the "checkm8" exploit may contain additional data including user-level activity. To understand what, if any, impact this would have on my original conclusions I obtained authorization to re-image and further examine Marcus Morrow's ("Defendant(s)") Apple iPhone 7 Plus.

SCOPE OF DIGITAL FORENSIC EXAMINATION

For purposes of this supplemental report, the scope of the digital forensic examination authorized by attorney Earl Houston is consistent with my September 9, 2020 report:

- Coordinate the forensic preservation of Marcus Morrow's Apple iPhone 7 Plus using a qualified digital forensics practitioner located near Mr. Morrow's Boone County, Kentucky residence
- Forensically examine a copy of the preserved Apple iPhone 7 Plus to determine if Mr. Morrow's phone was in use between 1:00 AM and 1:40 AM Central Daylight Time (CDT) on April 11, 2019, referred herein as the Period of Interest
- Determine if the phone was in use at or about the Reported Time of the accident, 1:43 AM according to the State of Mississippi Uniform Crash Report
- Assess the mobile phone for any indication of spoliation
- Examine the phones, documents and records associated with the Plaintiffs in this matter

DIGITAL FORENSIC PRESERVATION

Forensic Preservation

As Mr. Morrow lives in Boone County, Kentucky, Memphis-based Verity Digital Forensics again selected One Source Discovery in Louisville, Kentucky to perform the checkm8 extraction. One Source Discovery successfully obtained the checkm8 extraction using the Cellebrite "Universal Forensic Extraction Device" (UFED). A copy of the preserved evidence was made available by One Source Discovery to Verity which I downloaded to my forensic workstation. My examination was performed on a copy of the forensically extracted evidence.

DIGITAL FORENSIC EXAMINATION PROCEDURES

This section summarizes the procedure I used to decode and examine the checkm8 extraction obtained by One Source Discovery from Marcus Morrow's mobile phone. My examination is performed on a copy of the forensically extracted data to ensure no changes are made to the original data extraction.

The Scope of Digital Forensic Examination was defined by attorney Earl Houston, counsel for the Defendants as noted on the previous page. During the examination I used a licensed copy of Cellebrite's Physical Analyzer software which is designed to decode or parse the data preserved by One Source Discovery.

DIGITAL FORENSIC EXAMINATION FINDINGS

The remainder of this report details the items identified during the examination as being of an evidentiary nature in the examination requested by attorney Earl Houston.

All evidence recovered and documented herein was recovered from secondary storage (hard disk and/or non-volatile memory). No evidentiary data was acquired or intercepted during transmission or while in use by the user.

Call Logs

According to the Call logs recovered from the checkm8 extraction no additional calls were found to have been placed or received on April 11, 2019 between 1:00 AM and 1:40 AM.

iPhone Messaging

There are (3) types of messaging that may be recovered during a forensic examination of an Apple iPhone which Cellebrite Physical Analyzer software historically identified separately as Chat, SMS and MMS messages. Starting with Cellebrite Physical Analyzer v 7.28 these (3) messages types are now grouped together on reports as "Native Messages."

EXHIBIT A depicts the messaging history recovered by the checkm8 for the period of interest. I have added two columns, a reference number (REF#) and cross-reference (XREF) which correlates the message back to its original message type in my original report.

According to the messaging recovered from the checkm8 extraction no additional messages were found to have been sent or received on April 11, 2019 between 1:00 AM and 1:40 AM.

Internet History

According to the Internet history records recovered from the checkm8 extraction no Internet History was was recovered for April 2019.

Social Networking Apps

My examination shows that no social networking apps were in use on Mr. Morrow's iPhone on April 11, 2019 between 1:00 AM and 1:40 AM.

knowledgeC Database

The knowledgeC database, available with the checkm8 extraction, stores the event logs of running processes on an Apple device and can be used to ascertain user-level personal activity, also known as "pattern-of-life analysis." This could show how a user was interacting with their phone and may include, but is not limited to, timing around activities such as: device lock/unlock; login events, the installation and use of particular apps; spotlight searches; screen status and more.

My examination of the knowledgeC database and related artifacts on Mr. Morrow's iPhone does not show any user-level activity on April 11, 2019 between 1:00 AM and 1:40 AM other than what was noted in my September 9, 2020 report.

checkm8

I concur with Plaintiff's expert Larry Daniel that the checkm8 extraction provided considerably more data than the Advanced Logical, however upon my examination there was nothing recovered that would alter my original conclusions.

CONCLUSION

To the best of my professional knowledge, and to a reasonable degree of digital forensic certainty, I continue to believe that:

- Though the recovered call logs from Mr. Morrow's iPhone did not extend back to the date of the accident, according to the phone records provided by Sprint, other than the 1:36 AM call to 911, no other calls were placed or received during the period of interest identified by counsel.
- Twenty-four (24) minutes prior to the 911 call, a single MMS message having an attachment attempted to send at 1:12:28 AM. A few seconds later the same attachment was successfully sent as a Chat (iMessage) message at 1:12:42 AM. No other MMS or Chat messages were exchanged during the period of interest.
- No SMS messages were sent or received from Mr. Morrow's phone on April 11, 2019 between 1:00 AM and 1:40 AM.
- No Internet history records were recovered for April 2019. The majority of the records that were recovered were in a deleted or unknown status. When browsing the Internet Mr. Morrow may have used the Private Browsing feature of his browser and/or he may have deleted his Internet History.
- No social networking apps were in use on Mr. Morrow's phone on April 11, 2019 between 1:00 AM and 1:40 AM.
- The dash cam video from the accident further confirms what I found during the forensic examination of Mr. Morrow's Apple iPhone 7 Plus, he was clearly not interacting with his phone at the time of the incident.
- The 911 call placed by Mr. Morrow at 1:36 AM is the closest activity on his iPhone that I could find in relation to the time of the accident.
- Additional information in the form of deposition transcripts, documents, records, and mobile forensic data extractions from the Plaintiffs' phones and social media accounts are required.

EXPERT QUALIFICATIONS

I have been a Partner and Lead Examiner at Verity Digital Forensics since 2004 and have over 25 years of experience in the Information Technology field. My expertise is in digital forensics including data acquisition and imaging, litigation project support and data recovery.

I am recognized as a Certified Computer Examiner (CCE) by the International Society of Forensic Computer Examiners (ISFCE). I also maintain the Project Management Professional (PMP) credential through the Project Management Institute (PMI).

This work is based on information known to me and may be supplemented if additional relevant information becomes available.

The only work contemplated but not yet completed, is the preparation of possible demonstrative exhibits, and, if engaged to do so, preparation to testify and attendance at depositions and trial.

I reserve the right to amend, revise or further supplement my findings as further information becomes available. The includes but is not limited to documents, records, mobile forensic data extractions and forensic examination of the Plaintiffs' mobile phones and social media accounts

Ted R. Scott, CCE
Lead Digital Forensic Examiner
Verity Digital Forensics

November 16, 2020